

**Cyberspace Technological Standardization:
An Institutional Theory Retrospective on the Generation Edge***

By: Daniel Benoliel**

Note - In compliance with the conference's space restrictions, the present version was shortened and includes parts: I, II, V.d & VI. This document also contains the table of contents of the full document. For the full version of this paper, please visit: <http://www.ocf.berkeley.edu/~dbenolie/cyberspace_technological_standardization.pdf>.

ABSTRACT

The Clinton administration originally had made 'industry self-regulation' its guiding principle for standardizing cyberspace. So far, this principle has not been changed by the succeeding administration. This paper is a historical and conceptual assessment of that policy, examined through the prism of comparative institutional theory.

Historical analysis of the last two decades shows that industry 'self-regulation' was not always a coherent policy but sometimes a rhetorical device used to legitimize the government's own agendas. Such as, cyberspace's architecture and infrastructure mandated design. Thus far, there are still far too many inconsistencies in its formal standardization policies. The intentions, actions and declarations aimed at further privatizing the net's funding and governance - on the one hand, as can be seen in the quasi-privatization of the Internet Corporation for Assigned Names and Numbers (ICANN) case study; On the other hand, the practice of offstage standard centralization of establishing early policies for infrastructure standardization.

Consideration of cyberspace's multi-layered architecture, will attempt to answer the comparative institutional question of 'who should standardize the net?' This question would be then subject to the distinctive production process of cyber standards. Thus, distinguishing between early infrastructure standardization on the one hand and complementing application standardization on the other. This is in reference to the FCC's incomplete legal category definitions.

This study will conclude with a set of comprehensive policy rules backed by a caveat; as with analogous IT standardization regimes, unless distinctive standardization categories and policies will not be maintained en bloc and thus sequentially and context-based – cyberspace's present relatively successful institutional regulative reality may not always be preserved effectively also prospectively.

TABLE OF CONTENTS

I. Introduction.....	4
II. The technological triple scrutiny analysis.....	11
A. General.....	11
B. Information technology (IT) standards – The methodological framework.....	11
C. The technological life cycle: The criterion of ‘time’.....	12
D. Cyberspace’s architectural edifice: The criterion of ‘space’.....	15
1. General.....	15
2. Infrastructure Standards.....	19
3. Application standards.....	22
E. Standard setting institutions: The criterion of institutional identity.....	23
F. Conclusions.....	26
III. The Development phase: The political institutional inevitability.....	27
A. General.....	27
B. Infrastructure telecommunications services: the collective choice analysis.....	27
C. Infrastructure Standardization: the cost-benefit analysis.....	35
1. General.....	35
2. Administrative costs.....	37
a. Quality standardization costs.....	37
b. Development costs.....	40
c. Convey information about standards.....	41
3. Compliance costs.....	42
a. Coordination costs.....	43
b. Reduce inefficient variety costs.....	45
4. Indirect costs.....	45
IV. The Modification phase: The commercialization of cyber standards.....	47
A. Overview.....	47
V. The Implementation phase: The rise of autonomous institutions.....	52
A. General.....	52
B. Application standardization: the cost-benefit analysis.....	52
1. Administrative costs.....	53
a. Eliminating duplicative efforts.....	53
b. Reduce search costs.....	55
2. Compliance costs.....	56
3. Indirect costs.....	59
C. Government intervention.....	60
1. General.....	60
2. Direct intervention: The problem of efficiency.....	61
3. Indirect intervention: Roles of government regulation.....	63
a. General.....	63
b. Regulate production supervision rules.....	65
c. Regulate the process of standardization.....	68
D. A potential deviation: The ICANN case study.....	70
VI. Conclusions.....	76

I INTRODUCTION

One of the most consequential ways to regulate cyberspace and shape its markets is by technological standard setting.¹ Seen too often as a gray and overly technical discipline, it is mistakenly, also a mostly neglected field of research on cyberspace regulation: That is, both as an independent field of regulation theory, and more specifically, as seen through the prism of institutional governance in cyberspace.

As with other technological fields of mass media standardization, i.e. broadcast, cable and satellite, TV and radio - cyberspace seems to have reached the degree of comprehensiveness, so as to be worthy of a wider perspective of comparative institutional analysis – wider than the one suggested by the U.S. government in its arguably nonexclusive category definitions.² Thus far, there is still too much ambiguity and inconsistency in its regulation (i.e., standardization) policies in cyberspace: intentions, actions and declarations aimed at further privatizing the net's funding and governance, on the one hand, as can be seen e.g., through the Internet Corporation for Assigned Names and Numbers (ICANN) self-regulation case study; And centralization and even natural monopolization of standard setting activities of *infrastructure* standardization, on the other.

* © 2002 Daniel Benoliel.

** J.S.D candidate, UC Berkeley, School of Law (Boalt Hall). This paper won the first place in the 30th Telecommunications Policy Research Conference (TPRC 2002) student article's competition. For their most helpful comments and support, I am indebted to Mark Lemley, Pamela Samuelson, Edward Rubin, David Post, Stuart Benjamin, Hal Varian, Dan Hunter, Polk Wagner and Jane Winn. I am also grateful for the generous advice I received from Carl Cargill and Roger Martin from Sun Microsystems, Inc. Any inaccuracy would be my responsibility. For further questions or comments, please email me at: Daniel_b@boalhall.berkeley.edu.

¹ On the standardization discipline as an independent form of regulation, see, e.g., S. Breyer, *Regulation and Its Reform* (Harvard University Press, 1982) (for an economical perspective), p. 96 et al.; A. Ogus, *Regulation: Legal Form and Economic Theory* (Clarendon Press: Oxford, 1994), p. 150 et. al, and Fn. 1 & accompanying text; See, also, C. F. Cargill, *Open systems standardization: A business approach* (Prentice Hall PTR, 1997) (for an information technology perspective), pp. 26-29, 137-138; J. R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553, pp. 570-572 (for the cyberspace context) [Hereinafter, *Lex Informatica*]; J. R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 Emory L.J. 911 (concluding that standards in cyberspace embed policy choices, thus supplementing legal rules), pp. 918, 927-928.

² On the need for technological comprehensiveness for standard setting, see, e.g., Martin C. Libicki, *Information Technology Standards: Quest for the Common Byte*, (Digital Press) (1995) (on the need for proper level of comprehensiveness in standard setting), pp. 16-18; T. M. Egyedi, *Institutional Dilemma in ICT Standardization: Coordinating the Diffusion of Technology*, 48, In *Information Technology Standards and Standardization: A Global Perspective* (K. Jakobs, ed.) (IDEA Group Publishing, 1999) (on the advanced need for implementation-dependent solutions for Internet standards, even more so than in other information technologies fields), p. 57; Ole Hanseth & Eric Monterio, *Participatory Standardization of Information Infrastructure*, In *International Perspectives on Information Systems: A Social and Organizational Dimension* (Savvas Katsikides & Graham Orange, eds.) (1998) (“The only general purpose information infrastructure in widespread use is Internet”), p. 174.

With the commercialization of the net and the development of peripheral standardized software products, based on technological infrastructure platforms, the question of ‘who should standardize the net?’ can now be learned not only from experience of analogous technological fields, but ultimately also from within its own retrospective experience of mainly the last two decades.³ This study attends this ‘call of arms’, while confronting the unique progress of what is, in essence, a technological standardization process.

As an institutional policy question, this study departs from Neil Komesar’s comparative institutional theory insight: Acknowledging that all standardization institutions are subject to both internal and external imperfections - only a comparative approach vis-à-vis the identical assignments that should arguably prevail.⁴ Accordingly, whenever any institution may function inefficiently, alternative institutions may function even worse. By the same token, whenever the intrinsic worth of any institution might be apparent, alternative institutions may perform the same task even more effectively.⁵ For example, upon examining market ability to self-standardize cyberspace, the operative question is not how well the market functions, but whether political institutions, i.e. government branches and/or other autonomous institutions e.g., industry standardization organizations, could produce a better outcome and should therefore prevail.

In doing so, this study will focus predominantly on the relationship between institutional analysis and standardization *production* policy as an ex-ante regulative mechanism. That is, instead of the more common concern about the ex-post antitrust and intellectual property legal implications of telecommunications regulation; or the traditional described relationship between commercial implementation of a new technology on *content* of legal (but even technological standards), as can also be viewed through the more general prism of regulation theory in cyberspace.⁶ In the latter forms of discourse, any institutional choice is mostly a

³ On the importance of precedents in designing standardization policies, see, e.g., S. Breyer, *supra* note 1, p. 99; Jason Oxman, *The FCC and the Unregulation of the Internet*, Counsel for Advanced Communications, (FCC OPP, Working Paper No. 31, 1999), at: <http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31> (last visited 28 August 2002) (“Where the distinction blurs between the regulated and the unregulated, between traditional categories of service and new methods of delivering traditional services...[T]he Commission should be guided by the last thirty years...”), p. 24; Kevin Werbach, *Digital Tornado: The Internet and Telecommunications Policy* (FCC OPP Working Paper Series 29, March 1997), at: <http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf> (last visited 28 August 2002), p. 26. In balance, Werbach warns us that there are reasons to believe that such analogies to familiar services may not be appropriate for the Internet due to real ‘category’ difficulties, *id.* Henceforth, any such analogy will derive from the proposition of contextual analysis, unless claimed otherwise.

⁴ Neil K. Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (1994), pp. 3-10.

⁵ *Ibid.*, *id.*

⁶ So far, the latter prism is to be found in the core of the ongoing debate regarding application standards i.e. user-oriented software - as a regulative constrain, thus overshadowing the separate debate concerning system-oriented infrastructure standards. See, e.g., L. Lessig, *Code and Other Laws of Cyberspace*, (basic books, 1999) (explaining that his book and the present regulative discussion is (and should be) aimed at the standardized application layer), pp. 101-102; See, also, D. R. Johnson & D. G. Post, *Law and Borders--The Rise of Law in Cyberspace*, 48 *Stan. L. Rev.* 1367 (1996) (examining standardized applications e.g., copyright and trademark regimes as the point of reference in their regulative argument), pp. 1382-1391; Timothy Wu, *Application-Centered Internet Analysis*, 85 *Va. L. Rev.* 1163 (1999) (“[t]he whole Internet is

reflection of an earlier pursued policy or defined 'rights', i.e. Lessig's constitutional urge for reducing 'code control', or Post's freedom for regulative multiplicity.⁷ Seen from an institutional perspective, that discussion seems to be largely characterized by its placing of legal and other normative principles above the political *production* process and costs.

The Komesarian proposition, on the other hand, suggests that the mere reflection of any social goals and 'rights' on institutional choices are largely insufficient, as they tautologically imbed institutional choices of their own.⁸ Accordingly, any social policy should become relevant only upon an earlier consideration of the proper institutional constraint.⁹ In agreement with this line of thought, this study will suggest that any institutional choice should be seen, in essence, as an integral part of the general technological (and thus, social) goal and not solely its mere reflection.

Based on this proposition, this study will describe what ought to be viewed in future technological generations of cyberspace - a new multi-layered production process of technological standardization. Thus, offering an alternative synthesis to the existing top-bottom, bottom-up and industry standardization organization's single-layered regulation models¹⁰; that, as a general matter, seem all to fall short regarding the notable factor of *timing*.

As a reflection of the processional nature of this technological environment, the strength and weaknesses of one model versus another, will be measured in each sequential phase, as they may vary in both space, i.e. types of standards located on different layers of architecture, and from one production stage to another. Overall, the institutional choice between these different standard setters for each phase will be only a transitory choice among highly imperfect alternatives.

rarely an appropriate level on which to generalize. Instead, legal thinking can better focus on where the variation that is apparent to the user is actually found: the application layer above the Internet's basic protocols"), p. 1164; Llewellyn J. Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 Cornell J. L. & Pub. Pol'y 475 (1997) (using the term cyberspace 'infrastructure' while focusing on 'application' standards instead e.g., email systems, World Wide Web, etc), pp. 481-487; Dan L. Burk, *Federalism in Cyberspace*, 28 Conn. L. R. 1095 (1996) (focusing on consumer protection applications and other public laws to police online behavior and commerce).

For a skeptical view of this trend, see, e.g., Carl Shapiro and Hal R. Varian, *Information Rules: A strategic guide to network economy* (Harvard business school press, 1999) (suggesting that "the Internet infrastructure is bound to become more regulated in the years ahead"), pp. 317-318.

⁷ L. Lessig, *Ibid*, id; D. R. Johnson & D. G. Post, *Ibid*, id, respectively.

⁸ Neil K. Komesar, *supra* note 4, ("calling something a 'right' is an institutional statement"), p. 43.

⁹ *Ibid*, (firmly suggesting that "the choice of social goals or values is insufficient to tell us anything about law and public policy either descriptively or prescriptively. One must seriously consider institutional choice in order to understand or reform law and public policy"), p. 271.

¹⁰ Neil K. Komesar, *supra* note 4 (suggesting that, originally, the available institutions are political institutions i.e. executive and legislative branches of government, market and the courts), e.g., p. 6. However, cyberspace technological environment embed, in practice, additional autonomous institutions i.e. industry, group consortias, etc, while minimizing the role of courts, as will be explained in § II.E, *infra*. For now, see generally, e.g., J. Farrell & G. Saloner, *Competition, Compatibility and standards: The Economics of Horses, Penguins and Lemmings, Product standardization and Competitive Strategy* 1 (H.L. Gabel ed., 1987), p. 1 et al.

Lastly, with the purpose of comparing institutions, Komesar's position initially relies on a public choice legal process analysis.¹¹ That is, according to both the relative value of institutions, based on the levels of participation allowed by them, along side with their inherent participatory processes imperfections.¹² Nevertheless, for cyberspace's technological setting, this study will also confront the distinctive costs of standardization, which are to be found outside the partial scope of its institutional participatory process. Another presiding premise would, therefore, suggest that any institutional choice should be also subject to production costs that exist beyond the participatory process per se. That is, whenever strict legal process analysis falls short in supplying policy makers with a comprehensive result.¹³ This study will, therefore, depart from the supported proposition that current law and economics, same as public choice and interest group theory, may be seen to share a joint objective and importance in standardizing cyberspace – as would be examined through the proper institutional analysis hereinafter. As a result, a preliminary cost-benefit analysis would be generally outlined in parts III-V, all in the following order.

Part II opens with a lead up description of the three technological benchmark criteria of the standardization realm. It upholds a conceptual definition of an IT standard, as a function of both technical maturity and commercial acceptance. Later on, this designation will also define the scope of the following discussion, as to exclude “non-standard” technology from the following policy discourse. Accordingly, a descriptive framework of the three standardization constrictions of: time, space and institutional identity - referring to the questions of ‘when?’, ‘what?’ and, ultimately - ‘who?’ can standardize, would be set up, respectively. In accumulation, all three define a triple scrutiny test bed for the competing standardization institutions in cyberspace. Methodologically, in the following parts both the criteria of space and institutional identity would be dealt through the third prism of the different standardization phases, as follows.

Part III begins with the first among three – ‘development’ phase. In this early technological phase, new platform technology is typically introduced, beginning with it's generation from an idea to the development of a basic system product or process, thus creating the content of the first standardized core or infrastructure technology. In this early technological phase a theory of central political institutional inevitability i.e. mandated government intervention in infrastructure standardization will be upheld.

In retrospective, it will be suggested that apart from its self-regulation rhetoric - the U.S. government was justified in taking a dual regulative attitude towards what were two main

¹¹ Neil K. Komesar, *supra* note 4, pp. 53-58, 65-67, 128-138.

¹² *Ibid*, id.

¹³ On the accumulative need for production costs, see, e.g., Edward L. Rubin, *The New Legal Process, the Synthesis of Discourse, and the Microanalysis of Institutions*, 109 Harv. L. Rev. 1393 (1996) (supporting a comprehensive synthesis to law and economics and the legal process movements for comparative institutional analysis), pp. 1394, 1411-1413, 1425-1437. See also, James G. March & Johan P. Olsen, *Rediscovering Institutions* (1989), pp. 1-2, 16-19; Paul J. DiMaggio & Walter W. Powell, *Introduction to The New Institutionalism in Organizational Analysis* 1 (Walter W. Powell & Paul J. DiMaggio eds., 1991), p. 11-15; Neil K. Komesar, *Exploring the Darkness: Law, Economics, and Institutional Choice*, Wis. L. Rev. 465 (1997), pp. 466-471.

distinctive purposes.¹⁴ The first, as would be generally described through a broad cost-benefit analysis, was the central initiative to unify cyberspace's standardized infrastructure, namely - both the worldwide domination of the compatible TCP/IP set of protocols, along with the formal adoption of cyberspace's hierarchical multi-layered architecture.

Only, with what was a successful achievement of this early standardization goal, did the U.S. government continue to its second substantively different goal, namely - the gradual transfer of power over the Internet backbones into new market agents, namely - the predominant stakeholder interest groups of the traditional common carrier telecommunications and cable industries.¹⁵ Conversely, for the latter objective, as will be critically evaluated through Olsen's 'collective choice' theory, the government rightly restrained itself into an indirect monitoring role to gradually encourage these interest groups into seizing control over growing larger backbone levels, in part or in full.

Part IV continues to the 'Modification' phase and explains how rapid innovative changes, through which cyber technology has undergone, was followed by extensive bargaining over technological change and later - commercial modifications as will be analyzed shortly. These changes are what, in essence, suggested to have led to the third and present commercial standardization phase.

Part V describes this concluding technological 'Implementation' phase. As it will be argued, whenever technology matures, the diffusion of new markets for both early core Internet telecommunications services and markets for application and conforming standardized products evolve - and should promote the raise of autonomous standard setting institutions. For that matter, four consecutive arguments will be raised. First, with the growing concerns about governmental 'technological bias' through cyberspace standardization policy-planning and 'code control', formal industry standardization is, arguably, the most efficient institution in chilling direct governmental incentives for intervention, beforehand or ex-post, as it is in chilling of anti-competitive market standard setters motivations. Upholding this comparative institutional argument - an updated cost-benefit analysis of the different commercial standardization costs i.e. administering, compliance and indirect costs for manufacturers and other agents, will be met.

Second, it will be further argued that apart from the limited *infrastructure* maintenance standard setting activity of the present phase, e.g. increase in bandwidth on the backbone

¹⁴ For a description of secondary standardization policies, see, generally, e.g., Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, Stephen Wolff, *A Brief History of the Internet* (2000) <<http://www.isoc.org/internet/history/brief.html>> (last visited 28 August 2002) [Hereinafter, "Brief History"], p. 8-9.

¹⁵ The Telecommunications Act of 1996 adds the broad related category, "telecommunications" service, defined as follows: The term "telecommunications" mean the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. 47 U.S.C. §153(43). [Hereinafter, "The Telecommunications Act"]. The term "telecommunications service" means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available to the public, regardless of the facilities used. 47 U.S.C. §153(46). As for the category difficulties this definition creates for Internet standardization purposes, see, also, the discussion at § II.D.2, *infra*.

transmissions links, better physical access from homes and businesses or even a more sophisticated network architecture - a government should restrain its former direct role from standardization activity, allowing Internet telecommunications providers and application standard setters to be constrained only ex-post by market forces, met by intellectual property and antitrust law.

Third, the *indirect* governmental standardization policy should then be promoted through two groups of proactive roles. The first, regulate supervision rules, which facilitate market production of standards by market agents. The second is to regulate procedural rules for the standardization process aiming at further confirming the legitimacy of both standardization decision-making and its outcomes. These technological policies will be examined, accordingly.

Fourth, it would be argued that one potential deviation from the supported general governmental policy for infrastructure standard setting may come in the form of the federal government involvement with the ICANN 'domain name system' (DNS) governance. Originally, the question of technological standardization was not raised properly as a policy question, thus undermining the need to decide on technological policy risks. In fact, it would be suggested that ICANN's technical mandate reaches potentially much further than might be literally understood from the varied formal documentation. Seen too narrowly as mere technological routine standard setting maintenance, it would be further argued that because no governmental guidelines were adequately established, the necessity for a visible and continuous technological standardization policy was potentially undermined (at least for infrastructure standardization as will be suggested beforehand, in part III.B) – as can be seen through the emerging institutional risk of self-standardizing the DNS.

Part VI will deduce several conclusions, which are suggested as policy rationales for future technological generations in cyberspace. The main conclusive proposition will be that the unprecedented development of cyberspace seems to provide theoreticians and decision-makers alike, i.e. FCC regulators, with a unique opportunity to develop a comprehensive, and thus chronological and context-based institutional standardization policy. This is in accordance with the different consecutive production phases and types of standards that result from this new technological realm vis-à-vis the U.S. government and FCC's existing legal framework.

Upon choosing the optimal standardization institution for each technological phase, the significance of this observation for the purpose of institutional theory in cyberspace, would arguably, be threefold. First, once different phases of technological development along with standardization institutions, which affect the market differently - are recognized, a rational standard setter would be also able to predict efficiently, the degree of compliance of each such standardized technology with a user-oriented competitive analysis, if at all. Second, the raise of different types of IT standards may then demand transitory regulatory conducts. Third, and ultimately, a comprehensive institutional framework could then be established for future technological generations in cyberspace. Establishing such framework is also the purpose of this study.

II THE TECHNOLOGICAL TRIPLE SCRUTINY ANALYSIS

A. General

Trying to narrow the conceptual framework to cyber standardization - a preliminary description of IT standards, should be agreed upon. Based on that, the three facets of cyberspace's standard setting environment i.e. time – referring to the professional technological life cycle; space – referring to cyberspace architecture, established by different types of standards; and, finally, institutional identity – would be described hereinafter. In accumulation, all three would suggest a triple scrutiny analysis for the appropriate institutional choice in each of cyberspace's distinctive standardization phases (as will be implemented in the following III – V parts). Ultimately, as will be argued, these well-established technological criteria should then be acknowledged and processed into the FCC's incomplete legal category deliberations. Based on that, a contextual institutional standardization framework could then be finalized.

B. Information Technology (IT) standards – The methodological framework

Typically, the technical criteria used in defining an IT standard are in accumulation, twofold. First, technically, a technological standard is primarily viewed by the degree of its technical maturity. That maturity is most commonly viewed through the scope of a technological standardization process.¹⁶

Second, and as a reflection of the all-purpose standardization appraisal, i.e. institutional analysis, an IT standard is quantified as a function of its acceptance by the relevant market, such as the cyber market.¹⁷ Practically, this measurement is assessed through the intensity and

¹⁶ For a practical industry perspective upholding this policy, see, e.g., at the Internet Engineering Task Force (IETF), a major IT cyber standardization organization, at S. Bradner, *The Internet Standards Process -- Revision 3*, RFC 2026 (Network Working Group) (Harvard University, October 1996) at: <<http://www.ietf.org/rfc/rfc2026.txt>> (last visited 28 August 2002) (“Specifications that are intended to become Internet Standards evolve through a set of maturity levels known as the "standards track"). Eventually, the IETF defined these maturity levels as -- "Proposed Standard", "Draft Standard", and "Standard", (The Internet standards track), at sec. 4 [Hereinafter, “the IETF”]. See, also, J. Postel (Ed.), *Internet Official Protocol Standards*, RFC 1800 (Network Working Group & Internet Architecture Board) (July 1995), at: <<http://rfc.sunsite.dk/rfc/rfc1800.html>> (last visited 28 August 2002) (for an earlier description of the maturity levels), at sec. 4;

For a supporting governmental perspective, see William J. Clinton & Albert Gore Jr., *A framework for Global Electronic Commerce* (1997), developed by the White House with the involvement of more than a dozen federal agencies, (concluding that “Premature standardization, however, can "lock in" outdated technology”) available at <http://www.ecommerce.gov/framework.htm> (last visited 28 August 2002), at § 9 [Hereinafter, "The Report"]; Stewart Crawford-Hines, *Formal Technical Reviews, Across All Maturities, Institute for Zero Defect Software*, at <<http://www.izdsw.org/projects/FTR/maturity.html>> (last visited 28 August 2002).

For a theoretical perspective, see, e.g., T. M. Egyedi, *supra* note 2, p. 49; See, more generally, Floyd Wilder, *A Guide to the TCP/IP Protocol Suite* (Second Ed., Artech House) (1998), pp. 368-370.

¹⁷ For a practical perspective, see IETF, which grants the strongest status, “Internet Standard”, only to those specifications, which have already become widely adopted. See, IETF, *supra* note 16, § 4.1.3.

the width of its recognition. Ultimately, this means real exercise by users. Naturally, that estimation typically derives from the recognition that the specified protocol or service used provides significant personal and social benefits to cyber participants and market, respectively.

Obviously, not every technological specification meets both criteria.¹⁸ Any technological development that does not comply with both is generally regarded as a “non-standard” technology.¹⁹ Usually it would be lacking the minimum degree of acceptance, based on the assumption that, originally, such technology was intended to be put on the standards track by its developers.²⁰ Another type of “non-standard” technology is found in specifications, which were previously defined as standards, until they were superseded by a more updated typical standard²¹, or otherwise fell into abandonment or disuse by users.²² In short, only specifications, which meet both criteria, are commonly regarded as IT standards. As potentially cohesive and stable technologies, these standardized specifications are found, justifiably, also at the focal point for cyberspace’s institutional policy planning as a whole.

C. *The technological life cycle: The criterion of time*

In writings on information technology standardization, it is well accepted that the technical absorption of highly technological finished products (or routine product improvement processes²³), into common usage, imbedding one standard or a more complex group of standards²⁴, is neither immediate nor inclusive, but rather progressive.²⁵ Seen through a ‘production stage model’, there are, by and large, three consecutive independent technological phases, in the establishment of a standardized technology.²⁶ Jointly, all three are part of what is

For a theoretical Information Technology perspective see, e.g., C. F. Cargill, *Information Technology Standards: Theory, Process, and Organization* (Digital Press, 1989), p. 42; Martin C. Libicki, *supra* note 2, pp. 18-19.

For an institutional analysis perspective, compare: e.g., G. March & J. P. Olsen, *supra* note 13, pp. 50-52.

¹⁸ Examples for standards that failed to congregate wide acceptance are most of the ISO standards for data communications, and the IEEE 802.6 standard for Distributed Queue Dual-Bus data communications, IETF, *id.*

¹⁹ The IETF, *supra* note 16, at § 4.2.1-4.2.4.

²⁰ *Ibid.*, (“Specifications that are not on the standards track are labeled with one of three “off-track” maturity levels: “Experimental”, “Informational”, or “Historic”), § 4.2.

²¹ *Ibid.*, *id.*

²² *Ibid.*, *id.*

²³ On the difference between ‘product standards’ and ‘process standards’, see, Carl F. Cargill, *supra* note 15, pp. 59-61; Louis G. Tornatzky and Mitchell Fleischer, *The Processes of Technological Innovation* (1990), pp. 20-22; Manfred M. Fisher & Börje Johanson, *Networks for Process Innovation by Firms: Conjectures from Observation in Three Countries 261*, In *Patterns of a Network Economy: Advances in Spatial and Network Economies*, (Börje Johanson, Charlie Karlsson, Lars Westing, Eds.) (1993) 263, pp. 263-264.

²⁴ See, e.g., C. F. Cargill, *supra* note 1 (“usually quite a few standards will be invoked at once”), p. 142; A. Sloane, *The standards process: Tools and methods for standards tracking and implementations*, *Computer Standards & Interface* 22 (2000) 5-12, pp. 6-7.

²⁵ See, e.g., J. Farrell & G. Saloner, *supra* note 10 (for the technological standardization perspective), p. 3; Louis G. Tornatzky and Mitchell Fleischer, *supra* note 23 (for the wider technological innovation perspective), pp. 27-3; and see *Fn. 27, infra.*

²⁶ For the purpose of this study, only a production stage model will be discussed, in compliance with the public standardization production process perspective of this study. For one alternative model, see, e.g., Louis G.

also known as a technological life cycle - a metaphor that typically describes the evolution of standardized technology from its emergence to its technological maturity and unavoidable decline.²⁷ In essence, a technological life cycle interacts with the standard process through the life of each standard or group of standards jointly.²⁸ As will be described hereinafter, each such production phase is technologically distinctive. As such, they will arguably require a separate policy approach, and also a separate institutional choice, as will be explained later on.

Broadly, in its early ‘development’ phase, a new technological innovation is introduced, beginning with idea generation to the development of a basic product or process, thus creating the content of the standard. In this phase, a standard is specified also in its public form.²⁹ In this technologically oriented phase, any premature consumer-oriented price-based competition of technological knowledge is usually both technically premature and economically inefficient.³⁰ As a result, very little price-based competition transpires in this phase. In the development phase, radical innovations develop entirely new core standards.³¹ As a whole, these standards are oriented toward increased technological performance, rather than an immediate market need. As a general rule, as in cyberspace, core or infrastructure standards usually establish a

Tornatzky and Mitchell Fleischer, *supra* note 23 (discussing also a private user-oriented stage model and the interplay between both models), pp. 28-29.

²⁷ In IT standardization literature, a variety of overlapping phases of this process were so far suggested. For several three-phased processes, see, e.g., R. Mansell & R. Hawkins, *Old Roads and New Signposts: Trade Policy objectives in Telecommunication Standards*. In F. Klaver & P. Slaa (Eds.) *Telecommunication, New Signposts to Old Roads*, p. 45 et al.; (IOS Press, 1992) (Suggesting the planning, negotiation and implementation phases); [ISO80], *General terms and their definitions concerning standardization and certification, ISO guide 2*, Geneva, 1980 (for a formal definition of ‘standardization’ as a three-phase process of formulating, issuing and implementing); T. M. Egyedi, *supra* note 2 (Suggesting the developing, inventing and diffusing phases), p. 49 et al.; M. J. Bonino & M. B. Spring, *Standards as change agents in the information Technology market, Computer Standards & Interfaces* (1991) 12, pp. 97-107; M. B. H. Weiss & M. B. Spring, *Selected Intellectual Property Issues in Standardization, at Information Technology Standards and Standardization: A Global Perspective* (Kai Jakobs, eds) (Idea Group Publishing 1999), p. 63 et al.

For a variety of analogous five-phased processional descriptions, see, e.g., Y. Y. Sivan, *Knowledge Age Standards: A brief introduction to their dimensions, at Information Technology Standards and Standardization: A Global Perspective* (Kai Jakobs, eds) (Idea Group Publishing 1999), p. 1 et al. (Suggesting the missing, emerging, existing, declining and dying phases); For an economical perspective, see, also, S. Breyer, *supra* note 1 (upholding an analogous five-phased standardization process), pp. 101-109.

²⁸ See, e.g., C. F. Cargill, *supra* note 1, p. 142; A. Sloane, *supra* note 24, pp. 6-7.

²⁹ Hereinafter, regarded as the ‘development’ phase; See also, J.E.S. Parker, *The Economics of Innovation* 39 (1974), p. 48, Table 4.5; This dynamic correlation between the creation of innovations and standards is subject to a substantive change with the rise of standard commercialization, as will be described in § IV, *infra*.

³⁰ See, e.g., J. Gregory Sidak, *An antitrust rule for software integration*, Yale J. on Reg. (winter 2001) 1 (suggesting that “in such a market, consumer knowledge is accumulating, and product demand is still immature and unstable”), p. 27; Michael Whinston, *Tying, Foreclosure, and Exclusion*, 80 Am. Econ Rev. 837 (1990) (suggesting that lack of technologic maturity leads to unclear ex-ante results and to ambiguous future welfare effects), pp. 855-856; Carl Shapiro, *Antitrust in Network Industries*, (1996) at: <<http://www.usdoj.gov/atr/public/speeches/shapir.mar>> (last visited 28 August 2002) (The key driver of consumer benefits in information industries is technological progress), at sec III.A; See also the discussion in part III.B.2.a, *infra*.

³¹ Hereinafter, referred as ‘infrastructure’ standards.

necessary technical platform for future standardized applications and any other complementary standardized technologies.³²

In the second phase, the accepted technology generally undergoes rapid innovative changes. As competitors begin to challenge over consumer demands for enhanced complementing or application products and as extensive bargaining over modifications occur.³³ This arguably suggests a modification of the existing technical policies necessary for the emergence of new markets for core Internet telecommunications services and facilitating standardized applications. In the end of this phase the formal documentation of core-standardized technology is finally shared with the user community.³⁴ The modification phase also serves to enhance the creation of commercial products (or processes) that are to be finalized with the emergence of the following and last phase. In the intermediate modification phase no new type of standard is typically created.

In the last ‘implementation’ phase, due to technological and market limitations, technology matures, leading to the final diffusion of new markets for both core Internet telecommunications *services* and markets for application and conforming standardized *products*.³⁵ This activity typically propagates the unavoidable final decline of that same technology upon its standards, followed by the emergence of new product generations of a competitive nature (e.g., Internet Explorer (IE) generations).³⁶ In the third and last phase, complementary standards became largely oriented towards specific market needs of improving existing technology and further standardizing newer application and conforming standards.³⁷

As implied, in addition to the procession dimension of time, potentially, these different technological phases, may ultimately imbed the creation of substantively different types of standards.³⁸ Accordingly, as a function of both technological and commercial needs, several *categories* of standards emerge, as part of the overall technological standardization endeavor, and as such serve as an additional independent regulative constraint, as will be described for cyberspace, hereinafter.

D. *Cyberspace’s architectural edifice: The criterion of ‘space’*

1. *General*

³² This technological incentive is particularly effective when it creates entirely new markets for standards. The difficulty in maintaining this incentive after the development phase will be discussed in part V, *infra*.

³³ S. Breyer, *supra* note 1 (for a description of such bargains in various industries), pp. 107-108, 177-178.

³⁴ Hereinafter, regarded as the ‘modification’ phase.

³⁵ J. Gregory Sidak, *supra* note 30 (“In such a market, products are well-defined, both by the consumer demand that they satisfy and by the production technology through which firms supply them”), pp. 27, 28.

³⁶ See, generally, *supra* note 27, *id*.

³⁷ Hereinafter, referred as ‘application’ standards.

³⁸ See, e.g., L. G. Tornatzky & M. Fleischer, *supra* note 23, p. 165 et al.

Subsequent to evaluating the function of *time*, a rational policy planner should continue in evaluating the more long-established question of ‘*space*’, i.e. types of standards.³⁹ As will be described here, in cyberspace, that question would also be a function of architectural layer ‘location’. However, even with technological standards the need for this criterion is, to some extent, less obvious. On the one hand, any overly strict definition of standards by type may lead to technological rigidity, as it might inhibit potential standard setters from developing additional and/or cheaper alternative standards.⁴⁰ On the other hand, identification of standards by type may potentially lower administrative costs and thus, also diminish both technological and economical uncertainty.⁴¹ In balance, the latter notion upholding the criterion regarding types of standards has commonly prevailed, both in theory and in the FCC’s practice.⁴²

Thus, as early as 1966, the FCC opened the *Computer Inquiry* to study the interrelationship of computers and telecommunications technologies, and the use of computer-based services over telephone lines. The FCC Commission observed that “the growing convergence of computers and communications has given rise to a number of regulatory and policy questions within the purview of the Communications Act.”⁴³ These policy concerns still hold true today as they were more than three decades ago in the First Computer Inquiry.⁴⁴

Later on, in the second Computer Inquiry, the Commission reaffirmed its essential regulatory approach to the provision of computer data services, but improved its analysis.⁴⁵ By distinguishing regulated telecommunications services from unregulated data services, the Commission created the categories of *basic* services (renamed telecommunications services)⁴⁶

³⁹ See, e.g., A. Ogus, *supra* note 1, pp. 165-168.

⁴⁰ See, e.g., *Ibid*, p. 167.

⁴¹ *Ibid*, *id*. See, also, § III.B.2, *infra*.

⁴² However, due to the former argument’s practical constraint, only the main distinctive types of standards in cyberspace would be examined independently, hereinafter.

⁴³ See, *In the Matter of Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities*, 7 FCC 2d 11 (1966) (First Computer Inquiry), § 2 [Henceforth, “First computer inquiry”]. Overall, the three Computer Inquiries were a series of FCC regulatory proceedings that addressed the apparent convergence between telecommunications and computing. Although they partly influenced the Telecommunications Act, certain of their orders are still in effect, as will be described hereinafter.

⁴⁴ *Ibid*, *First Computer Inquiry*, *id*.

⁴⁵ This distinction was then formally adopted. See *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, Implementation of the Non-Accounting Safeguards of § 271 and 272 of the Communications Act of 1934*, as Amended, CC Docket No. 96-115, CC Docket No. 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, FCC 98- 27 (released Feb. 28, 1998) (“Use of CPNI”) at para. 46 (stating that telecommunications services and information services are “separate, non-overlapping categories, so that information services do not constitute ‘telecommunications’ within the meaning of the 1996 Act”).

⁴⁶ The Commission defined the term “basic” service, which referred to traditional common carrier telecommunications offerings as “the offering of transmission capacity for the movement of information.” *Computer II, Final Decision*, (Computer II Final Decision), 77 FCC 2d 584, at para. 93 (1980). The Commission defined “enhanced services” as: “...services, offered over common carrier transmission facilities used in interstate communications, which employ computer processing applications that act on the format, content, code, protocol, or similar aspects of the subscriber’s transmitted information; provide the subscriber additional, different or restructured information; or involve subscriber interaction with stored information”, see, 46 C.F.R. § 64.702(a).

and *enhanced* services (renamed information services).⁴⁷ The Commission also elaborated on the extent of structural separation required between the incumbent telephone provider and its enhanced services affiliate.⁴⁸

Foreseeing that the future would bring the convergence and interdependence of computers and communications, the Commission was also aware of the difficulty of separating the two into discrete categories:⁴⁹ On the one hand, as described earlier, the Internet in its contemporary form did not exist at the time the FCC formed the basic/enhanced distinction and as a result is still (partly) subject to genuine category interpretive ambiguities in the cyberian context, at least: For a start, and broadly put, as the Commission acknowledged with respect to the line it drew between the two services: "[p]lausible arguments can be tendered for drawing it elsewhere. At the margin, some enhanced services are not dramatically dissimilar from basic services or dramatically different from communications as defined in the first Computer Inquiry."⁵⁰ For example, appreciative data processing, computer memory or storage, or some advanced switching techniques typically identified as enhanced services, can be components of a basic service if they are used solely to facilitate the movement of information.⁵¹

Second, this FCC's classification has focused entirely on the issue from a telecommunications perspective. That is, with no adequate consideration of cable-provided Internet services.⁵² Instead, the Commission observed that because enhanced service was not explicitly reflected in the Telecommunications Act, there is no more a requirement to confront it with a specific

⁴⁷ The Telecommunications Act broadly defines an "information service", but excludes "telecommunications services" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service." See, 47 U.S.C. § 153(20).

⁴⁸ *Computer II Final Decision*, 77 FCC 2d, at paras. 190-266; For a wider discussion about the three Computer Inquiries' genealogy, see, Barbara Esbin, *Internet Over Cable: Defining the Future In Terms of the Past*, (FCC OPP, Working Paper No. 30, 1998), at: <http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp30.pdf> (last visited 28 August 2002), p. 25-26.

⁴⁹ See, Jason Oxman, *supra* note 3, p. 7; Kevin Werbach, *supra* note 3 ("[e]ven the premise that Internet services should not be regulated requires a precise assessment of what constitutes an "Internet" service...With the increasing prevalence of hybrid services, joint ventures, and alternative technologies, such distinctions will always be difficult"), p. 46.

⁵⁰ *Computer II Final Decision*, *supra* note 46, p. 434. In balance, the Commission avoided re-drawing the line at this margin due to its concerns that such action would potentially subject the issue to constant adjudication over the status of individual services offerings, *id.* However, as such distinctions are crucial for any institutional standardization analysis, such adjudication, is thus still necessary, and will be upheld in this chapter, hereinafter. See, also, Barbara Esbin, *supra* note 48 ("Regulators charged with implementing communications regulation find themselves unavoidably drawn into a process of determining the application or not, of existing rules whose terminology was established without regard to this new medium (The Internet, my emphasis, D.B.), for delivering communications services"), pp. i, 2.

⁵¹ *Computer II Final Decision*, *supra* note 46, p. 419-20.

⁵² Traditionally, cable service has been regulated as an integrated video, information content, and conduit service under Title VI to the Telecommunications Act. See, also, Barbara Esbin, *supra* note 48 (for an of integral cable-based analysis of Internet access services), pp. 3, 83-90, referring also to the *Report to Congress In the Matter of Federal-State Joint Board on Universal Service Under the Telecommunications Act of 1996*, CC Docket No. 96-45, FCC 98-67 (released April 10, 1998) ("Report to Congress"), where the FCC Commission expressly reserved for the future consideration of the "regulatory classification of Internet services provided over cable television facilities." Report to Congress, at para. 69 n.140, *id.*

traditional regulatory mechanism than there was for with cable television's formal elements of common carriage and broadcast television (then unregulated under the Act).⁵³

Third, to date, "advanced telecommunications and information services" as those terms are used in section 254(h) to the Telecommunications Act, have been interpreted to include also "Internet services". Internet services, regardless of the identity of the entity providing them, could also fall under the section 706 definition of advanced telecommunications capability," which is defined "without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics and video telecommunications using any technology."⁵⁴ Thus, even though the FCC has repeatedly found that the old regulatory categories are integral to the 1996 Act's new "telecommunications" and "information" service categories, as already explained, section 706 still seems to give the FCC a new and flexible, but nevertheless an indefinite regulatory category of "advanced telecommunications capability".⁵⁵ Moreover, anticipating future technological developments, section 706(b) also directs the Commission (and each appropriate State commission) to periodically initiate and complete inquiries concerning the availability of advanced telecommunications capability. In essence, disguised as a facilitating interpretive tool - section 706 should also be seen as an additional obstacle in the search of Internet conceptual clarity.

Fourth, even while upholding the Commission's policy to regulating only the common carrier *basic* transmission service, while exempting *enhanced* services from common carrier regulation⁵⁶, there is still little or no guidance in answering the question about how the Commission *should* act towards Internet-based services.⁵⁷ For standardization purposes, there was also no adequate distinction between the question of regulating enhanced *services* and that of regulating (i.e. standardizing) their own production. Thus, implicitly leaving also the latter criterion to the competitive 'hands off' premise of Title II of the Telecommunications Act.⁵⁸

⁵³ Thus, the second Computer Inquiry states: "Precedent teaches that the Act is not so intractable as to require us to routinely bring new services within the provision of our Title II and III jurisdiction even though they may involve a component that is within our subject matter jurisdiction". See, *Computer II Final Decision*, supra note 46, p. 430.

⁵⁴ Moreover, the use of "telecommunications" capability with no referral to any transmission media or specific technology raises the question of whether a new category of "broadband telecommunications" services that is different from either "telecommunications services" or "cable services" under the Act is therefore added to the above. That question, as well, albeit secondary in scope (potentially belonging to the basic services' carrying industries), still seems to add to the present categorical ambiguity.

⁵⁵ See, e.g., Barbara Esbin, supra note 48 ("The new statutory category of "advanced telecommunications capability," itself, which speaks not in terms of services and service providers, but of "capabilities," may arguably be utilized to develop a new regulatory framework better suited to fluid the types of communications capabilities made possible by the Internet"), pp. vi, 116; S. M. Benjamin, D. G. Lichtman, H. A. Shelenski, *Telecommunications law and policy*, (Carolina Academic Press, 2001) (for a description of a variety of technological services and products derived from § 706), p. 867.

⁵⁶ See, e.g., J. Scott Marcus, *The Potential Relevance to the United States of the European Union's Newly Adopted Regulatory Framework for Telecommunications*, at: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-224213A2.doc> (FCC OPP, Working Paper No. 32, 2000) (last visited 28 August 2002), p. 6.

⁵⁷ See, e.g., Kevin Werbach, supra note 3, p. 29.

⁵⁸ As mentioned earlier, the latter criterion of enhanced (i.e. application) standards' production will also be the focal point of the following III-V parts, infra.

Moreover, the Commission even went on noticing that it still maintains regulative jurisdiction over enhanced services under the ancillary jurisdiction of Title I, on the grounds that the enhanced services under consideration "constitute the electronic transmission of writing, signs, signals, pictures, etc., over the interstate telecommunications network".⁵⁹

Notwithstanding these interpretive difficulties, in the nowadays cyberspace these two dependent types of categories also give raise to two different types of standards. First, physical telephony infrastructure standards, supported by basic packet switching, transporting, addressing and routing standardized software (or protocols), which establish most of cyberspace's core or infrastructure standards. Originally, in the second Computer Inquiry and in subsequent orders, the Commission did come to address the implications of packet-switching technologies for this regulatory framework.⁶⁰ It was legally admitted that the use of packet switching and error control techniques⁶¹ "that facilitate the economical, reliable movement of [such] information [do] not alter the nature of the basic service".⁶²

Second, computer software products, which establish most of cyberspace's following application standards and are to be found in the user-oriented 'application' layer of cyberspace's architecture. Here as well, these functions involve substantial computer processing and interaction with customer-supplied information, information-processing functions, such as authentication, email storage and retrieval, Web page hosting, and domain name server lookups - and therefore fall squarely within the definition of enhanced services.⁶³ Specific enhanced services also include protocol processing and electronic publishing, as well as the provision of access to data networks such as commercial online services and the Internet.⁶⁴

Ultimately, both types of services upon their standards should, arguably, also pave the way for a more comprehensive and accurate multi-layered and standard-based understanding than the present one. That is, subject to the notion that the higher the layer and production phase are - the more specific the purposes of its standards become. Later on, with cleared categories, it will finally be possible to finalize the net's institutional regulative policy, at large (as will later be done in the following III-V parts).

⁵⁹ *Computer II Final Decision*, supra note 46, p. 432.

⁶⁰ For further discussion concerning the applicability of the basic/enhanced distinction to Internet telecommunications services, see Kevin Werbach, supra note 3, p. 31, referring to Robert Cannon, "What is the 'Enhanced Service Provider' Status of Internet Service Providers?" FCBA News, February 1997.

⁶¹ *Computer II Final Order*, supra note 46, p. 420.

⁶² For example, in subsequent decisions the Commission has determined that packet-switched networks following X.25 protocols, and frame relay service offerings, provide a basic transport service. See, *Application of AT&T for Authority under Section 214 of the Communications Act of 1934, as amended, to Install and Operate Packet Switches at Specified Telephone Company Locations in the United States*, 94 FCC2d 48, 55-57 (1983); *Independent Data Communications Manufacturer's Association, Petition for Declaratory Ruling that AT&T's InterSpan Frame Relay Service is a Basic Service*, Memorandum Opinion and Order, DA 95-2190 (released October 18, 1995); See, also, Kevin Werbach, supra note 3, p. 32.

⁶³ *Ibid.*, pp. 32-33.

⁶⁴ *Ibid.*, id.

2. *Infrastructure Standards*

In the face of the existing categorical ambiguity, technologically, cyberspace, and more distinctively, the Internet or the ‘interconnected networks’, are presently clearly and commonly defined by a unified architectural backbone structure and a unified set of core protocols, together known as the TCP/IP.⁶⁵ These refer to a large number of protocols that make part of the different levels of its standardized infrastructure technology. In general, the North American architecture, in connection with Europe through the EBONE communication supporter, consists of three autonomously managed levels of hierarchical standardized architecture, thus imbedding an independent data structure. Each of these levels represent a function performed when data is transferred between cooperating applications across the network, in the following hierarchical order: National Backbones (e.g., NSFNET)⁶⁶ which are attached among themselves, through (inter-) national network interconnections facilities, and down the line also to mid-level networks (E.G., Midnet), which are attached to local service providers (e.g., UCSD).⁶⁷

The latter backbone level is also ramified into five additional infrastructure standardized levels, beginning with different IP networks (e.g., 132.287.n.m), which are attached to IP sub-networks (e.g., 132.287.51.n), which are attached to IP Host/end-systems (e.g., 132.287.51.6)⁶⁸, which are attached to end-users (persons), which are attached to networked applications (e.g., X-Windows).⁶⁹

⁶⁵ A “backbone” is basically a telecommunications line (either owned or leased) that links one or more locations together.

⁶⁶ A ‘national backbone’ is one “maintaining a hub city in at least five different states, spanning both coasts, and peering at the major NAPS.” (*Boardwatch Magazine Directory of Internet Service Providers*, Vol. 2, Fall 1997, at 27).

⁶⁷ The FCC, which refers to cyberspace’s ‘lower’ physical telephony infrastructure through four physical categories, formally suggested an analogous definition: backbone, middle mile, last mile and last 100 feet. (*FCC Inquiry concerning the development of advanced Telecommunications, second report, FCC 00-290, 2000 WL 1199533 (2000)*). Being aware of the need for future flexibility, the additional definition of “Advanced telecommunication capability” was widely defined in the Telecommunications Act, section 706(c)(1), as to include ‘upper’ broadband telecommunications capability “using any technology”, i.e. cyberspace’s physical telephony infrastructure. In essence, the FCC regulators left this accompanying definition dynamic, so to have it adjusted in the future, stating that “future reports will reconsider it in light of changing conditions of both supply and demand...we may change the definition...we emphasize that our definition of advanced telecommunications capability will evolve over time”, *ibid*, § 14).

⁶⁸ A “host” is a computer directly connected to the Internet. Still, it does not accurately reflect the actual number of Internet users, and is usually shared by groups of users and is thus smaller than them in size.

⁶⁹ See, e.g., H.W Braun & K. C. Claffy, *Network Analysis for a Public Internet, In Public Access to the Internet* (B. Kahin & James Keller, eds.) (The MIT Press, 1995), pp. 353-356; Compare: Craig Hunt, TCP/IP: Network Administration (2nd Edition, O’reilly 1997) 1-22, 6, 8-9 (part 1) (for a functional-based description of the TCP/IP architecture in four levels only: “network access” (referring to the three backbone network levels); “Internet” (referring to the IP Networks and sub-networks levels); “host-to-host transport” (referring to the IP Host/end-systems) and the “application” level (referring to the end-users and the networked applications levels); For an analogous four-layer description, containing the Link, Network, Transport and Application layers, see ISO/OSI Network Model description, at: <http://www.uwsg.iu.edu/usail/network/nfs/network_layers.html> (last visited 28 August 2002). I will, hereinafter, suggest focusing on Hunt’s four labels and referring to them as layers. Previously, the Federal

Ultimately, the different layers also differ in their standardized system-oriented specifications. First, in the three backbone levels, consisting of the “network access” layer, very few protocols operate, as they handle relatively uncomplicated network interactions exclusively. This layer defines the network hardware and device drivers. As far as standardization matters, these ‘non-consumer-oriented’ levels include technologies for network management (e.g., the Simple Network Management Protocol (SNMP)⁷⁰, the Ethernet standard for local area networks⁷¹ and the Frame Relay packet-switched data communication service⁷²), standardized management interfaces for various classes of equipment (e.g., the Fiber Distributed Data Interface (FDDI) for the 100 Mbps local area networks⁷³), and other operations issues.

Second, more protocols exist at the next two levels up – the IP networks and sub-networks layers, or the “Internet” layer, where the IP protocol prevails. As a general matter, they are both responsible for routed data interchange between hosts and across network links, through addressing and moving of packets (e.g., the IP Version 6 standard (IPv6)⁷⁴), addressing-related issues (e.g., the Dynamic Host Configuration standardized Protocol (DHCP)⁷⁵), Open Shortest Path First (OSPF)⁷⁶ or the border Gateway Protocol.⁷⁷

Consecutively, the third and last infrastructure layer to follow is the “host-to-host transport” layer, referring to the IP Host/end-systems level. The function of this layer is to make the Internet more useful to its users and easier to use. This layer includes telecommunications and transport standardized protocols (e.g., the Transmission Control Protocol (TCP)⁷⁸), and more general standards for providing sufficient quality of service.⁷⁹

Networking Council (FNC) has unanimously upheld the existence of a layered architecture, as part of the Internet’s definition (“‘Internet’ refers to the global information system that...(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein”) (October 24, 1995). See, also, RFC 1958, B. Carpenter, *Architectural Principles of the Internet*, at, <<http://www.cis.ohio-state.edu/htbin/rfc/rfc1958.html>> (last visited 28 August 2002), pp. 2-4. The concluding networked standards layer, i.e. the application layer and standards, will be discussed independently, infra.

⁷⁰ Floyd Wilder, supra note 16, pp. 246-276.

⁷¹ Ibid, pp. 19-33.

⁷² Ibid, pp. 83-88.

⁷³ Douglas E. Comer, *Interworking With TCP/IP* (vol. 1: Principles, Protocols, and Architecture) (3rd ed., Prentice Hall) (1995), pp. 32-33.

⁷⁴ Floyd Wilder, supra note 16, pp. 155-164.

⁷⁵ Ibid, pp. 199-208.

⁷⁶ Ibid, pp. 213-226.

⁷⁷ Ibid, pp. 227-235.

⁷⁸ On the TCP protocol, see, Floyd Wilder, supra note 16, pp. 165-172; Carl Shapiro and Hal R. Varian, supra note 6, p. 237; See, also, the following Requests For Comments (RFC): *the standards "legislation" of the Internet*: RFC 793 (LAS) <<http://www.faqs.org/rfcs/rfc793.html>> (TCP) (last visited 28 August 2002); RFC 791 <<http://www.faqs.org/rfcs/rfc791.html>> (IP) (last visited 28 August 2002); RFC 894 <<http://www.faqs.org/rfcs/rfc894.html>> (Ethernet and IP) (last visited 28 August 2002); RFC 882 <<http://www.faqs.org/rfcs/rfc882.html>> (Name servers) (last visited 28 August 2002).

⁷⁹ This layer is generally dominated by two different protocols: YCP and UDP, which are responsible for negotiating the flow of data between any two network hosts. See generally, Floyd Wilder, supra note 16, pp. 163-164; Douglas E. Comer, supra note 73, pp. 179-190.

For an industry perspective on these layers, See, e.g., The IETF internal division, at <http://www.ietf.org>. For a list of dozens of working Groups in the mentioned areas, see, e.g., <http://ietf.org/html.charters/wg-dir.html>

As described, all of these three are breeding grounds for strict system-oriented standards, which together establish the net's infrastructure. As such they are also subject to separate standardization costs and as will be later argued - also a separate institutional choice.

3. *Application Standards*

On top of these three infrastructure layers comes the forth layer in hierarchy, namely the 'application' layer, referring to the end-users and the networked application levels of the Internet. The function of these standards is essentially twofold. For a start, as TCP/IP-compatible standards, they are developed in order to facilitate the operation of the infrastructure core standards. Such are the most familiar standardized network application protocols (e.g., the HTTP, FTP and SMTP, NFS, DNS, arp, rlogin, talk, ntp and traceroute).⁸⁰ These standards are also these that finally come to interact between clients (our personal computers) and the relevant data storage, namely the servers.⁸¹ A second application of these standards carries an independent innovative nature - With the emergence of new markets and sub-markets, as part of the variety of Internet computer software products, the application layer has given rise to: browsers, operating systems, encryption modules, contract infrastructures, electronic payment systems and security equipment (e.g., the IP Security (IPSec) protocols⁸² and XML Digital Signatures⁸³), X-Windows, Java, e-mail systems, etc.⁸⁴ In essence, application standards are distinct from infrastructure standards in both specifications and function. As user-oriented standards application standards as well, embed unique standardization costs and as will be argued accordingly – they ultimately imbed a separate institutional choice.

(last visited 28 August 2002); For a U.S. governmental similar perspective, see: *The Report*, supra note 16, § 9.

⁸⁰ Floyd Wilder, supra note 16, pp. 293-356; and see, also, Fn. 207 & accompanying text, infra.

⁸¹ Of central importance to this interaction are: HTTP (Hyper Text Transfer Protocol), which is also the most widespread used protocol in this layer, and is a protocol to publish (and read) hypertext documents across the Web; FTP (File Transfer Protocol), is a protocol for transferring files; SMTP (Simple Mail Transport Protocol), is a protocol for transferring electronic mail. Douglas E. Comer, *ibid*, pp. 344-347, 299-304, 315-323, respectively.

⁸² *Ibid*, pp. 471-488.

⁸³ See, e.g., *Extensible Markup Language (XML)* at: <<http://www.w3.org/TR/2000/REC-xml-20001006>> (last visited 28 August 2002).

⁸⁴ This same application layer lies also exclusively (and, arguably, only for the time being) in the core of the ongoing debate regarding application software as a regulative constrain. See, e.g., L. Lessig, supra note 6, pp. 101-102; D. R. Johnson & D. G. Post, supra note 6; D. G. Post, supra note 6; D. G. Post, supra note 6; Llewellyn J. Gibbons, supra note 6; Timothy Wu, supra note 6; Carl Shapiro & Hal R. Varian, supra note 6. Still, there are reasons to assume that this important debate will eventually expand, to the other infrastructure layers as well, only to follow the present cable and other telecommunications fields in and beyond the scope of software application standards, as will be upheld also in this study.

E. Standard setting institutions: The criterion of institutional identity

Finally, in the survey for the standard setting constituting criteria, lay its competing regulative regimes. Along with the criteria of timing of technological standard setting and space – referring to type of standards by location – this third criterion jointly suggests a three dimensional matrix of institutional choices, for policy makers to complete. Initially, institutions that regulate technological standards differ according to several variables. First, the degree of regulative formality, which evaluates the degree of legality and influence of its legitimate elective legislators. Turning to comparative institutional theory, March & Olsen address this question, while questioning both the primacy of such action and its outcomes.⁸⁵ Accordingly, the core task of political institutions is to confirm the legitimacy of choices made, by securing that relevant people are involved and by an appropriate control structure.⁸⁶ These same elements are arguably evident also in standardization ‘ideology’, as they define the role of formal standards bodies as guardians of the process.⁸⁷ Thus, standardization procedures should, eventually, serve also to legitimize the process of standardization. In all standardization bodies such specifications are just a starting point, and the ultimate test of a standard is whether it meets general acceptance, as suggested earlier. Functionally, standard setters carry also a role of checking the level of acceptance of their standards in relevant markets, i.e. cyber markets and sub-markets, through the intensity and width of their recognition and ultimately, through actual exercise by users. Measuring that acceptance typically derives from the recognition that the specified protocol or service used provides significant benefit to the cyber community and market.⁸⁸

Second, these variables also include the degree and type of monopolistic power over the right to supply, vis-à-vis the regulated status of all suppliers in a given market, as will be analyzed accordingly.⁸⁹ Third, the degree of their legal status, while evaluating their binding force and enforcement efficiency of a given standard.⁹⁰ As a general matter, such performance, in any event, is more difficult to monitor for several reasons. For a start, legally - in the United States there is no official means test for ascertaining whether or not a standardization organization is a formal or informal standard developer.⁹¹ Moreover, this differentiation is also blurred,

⁸⁵ G. March & J. P. Olsen, supra note 13, pp. 50-52.

⁸⁶ Ibid, id.

⁸⁷ See, e.g., Louis G. Tornatzky and Mitchell Fleischer, supra note 23, pp. 41-42.

⁸⁸ G. March & J. P. Olsen, supra note 13, id.

⁸⁹ See, e.g., *ibid*, id; Louis G. Tornatzky and Mitchell Fleischer, supra note 23, p. 41 (and Fn. 4 & accompanying text).

⁹⁰ Ibid, id.

⁹¹ In the United States alleged formal standards developers may request to be formally accredited by the American National Standards Institute (ANSI) (<http://www.ansi.org>) (last visited 28 August 2002). As part of both a non-binding and voluntary initiative, ANSI requires written procedures with strict requirements for openness, balance, consensus and other due process. Internationally, the situation is not substantively better off, as alleged formal standards developers may be created by declaration of treaty agreements between cooperative nations, such as the International Telecommunication Union (ITU) or by national policies which recognize a standards organization, such as the International Organization for *Standardization/International Electrotechnical Commission (ISO/IEC) joint technical committee, ISO/IEC JTC 1* (<http://www.jtc1.org/>) (last visited 28 August 2002). Draft of ‘International Standards’ adopted by the joint technical committee are

empirically - there being no experiments with competitive self-regulation, no real market for the *control* of standard setters; and no easy option of dismissal of ineffectual officials or even market standard setters by the principals (politicians and citizens).⁹²

Nevertheless, in practice, submitting to these characteristics, different types of standardization regimes were eventually characterized and defined as such. In one of the seminal articles on standardization, Farrell and Saloner identify what became commonly regarded as five distinctive types of such regimes, typically as a function of their standardization endeavors.⁹³ The first, and less influential in cyberspace, is standardization activity generated by internal decisions of autonomous firms i.e. whenever there is only one vendor.⁹⁴ Closely related to that is the second type of standards emerging from a mutual agreement among several manufacturers, whether formal or informal, binding and/or voluntary – aiming at finding consolidating potential different interests among the parties to the agreement.⁹⁵ Third, market *de facto* and industry *gray* standards could be developed and then absorbed by consumers through historical accidents⁹⁶, and more so by strategic choice of consumers in a competitive natural selection process, later to be adopted and dominate the entire relevant market.⁹⁷ This is made possible after such a standard achieves a predominant market share over potential competitors. These three formats are commonly known as informal standards (including *de facto*, *gray* or *ad hoc*⁹⁸ standards), and are produced by non-legally binding autonomous market forces (*de facto*) or even particular groups (e.g., non-profit organizations) or consortia (*gray*) standardizing autonomously.⁹⁹ Standards designed by *de facto* standard setters (but less

circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote. On the activities of ISO/IEC JTC 1, see, also, C. F. Cargill, *supra* note 1, pp. 200-204, 269-270.

⁹² See, e.g., J. Farrell & G. Saloner, *supra* note 10, p. 5.

⁹³ *Ibid.*, pp. 2-5; A. Ogas, *supra* note 1, pp. 108-109; M. A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 Conn. L. Rev. 1041, (1996) (focusing on the government, industry players and *de facto* standards); M. A. Lemley, *Standardizing Government Standard-Setting Policy for Electronic Commerce*, 14 Berkeley Tech. L. J. 745, 747; B. Toth, *Putting the U.S. Standardization System into perspective*, StandardView, 4(4) (for a review of the presiding organizations inside the U.S.), pp. 169-178.

⁹⁴ J. Farrell & G. Saloner, *supra* note 10 (concluding that a final analysis for both this regime and beyond is neither mutually exclusive nor independent), p. 2.

⁹⁵ *Ibid.* (adding that this type of standard setters face all the problems of autonomous firms, and more), *id.*; Carl Shapiro and Hal R. Varian *supra* note 6, pp. 236-237.

⁹⁶ See, Brian W. Arthur, *Competing technologies and lock-in by historical small events: The dynamics of allocation under increasing returns*, Tech. Rep. 43 Center for Economic Research, Stanford University, Jan. (1985) (modeling technological choice under increasing returns by consumers as a random process); Paul A. David, *Clio and the economics of QWERTY*, Am. Economic Rev. 75, 2, May 332-337 (further explaining the development of the type writer keyboard from this approach); Paul A. David, *Some new standards for economics of standardization in the information age*, In *Economic policy and technological performance* (P. Dasgupta and P. Stoneman eds.) (Cambridge University Press, 1987) (Further confirming Arthur's study on historical lock-in under increasing returns).

⁹⁷ See, L. M. Katz and C. Shapiro, *Network Externalities, competition and compatibility*, Am. Economic Rev. 73(3) June, 424-440; L. M. Katz and C. Shapiro, *Product compatibility choice in a market with technological progress*, Oxford Economic Papers 38 (Nov.) 145-165 (formalizing Arthur's notion (see Fn. 96 above) into a theoretical model describing consumer's choice of technological products as a strategic consideration).

⁹⁸ For a preliminary description of Ad Hoc standard setting activity and institutions, see, e.g., Martin C. Libicki, *supra* note 2, pp. 18-20.

⁹⁹ In few cases, companies may operate outside the established standard-setting organizations in consortia to form standards. For a preliminary description of consortia, see, Roy Rada, *Consensus versus Speed*, In

so, gray standards) are typically driven by self-interested implementers and tend to be both proprietary and close. Consequently, they are especially interesting legally, for the reason that particularly in the implementation phase they tend to raise a variety of issues concerning the proper scope of antitrust and intellectual property law in influencing market outcomes.¹⁰⁰

A fourth type of standardization institutions is government, usually through delegated regulatory agencies or organizations. The standards they produce are typically made to serve, and thus penetrate an entire industry. Finally, standards introduced by intra-national, and more so, international standardization organizations operating jointly, through special agencies.¹⁰¹

These last two regimes are commonly known as formal (*de jure*) standards and standard setters. They are processed by traditional political standard development organizations, such as the International Organization for Standardization (ISO), Internet Engineering Task Force (IETF) etc., scientific or professional societies, trade associations or other types of industrial standard organizations, which may operate in accordance with official formal regulative bodies.¹⁰² Historically, in other fields of media, standardization used to be the prefecture of international industry standardization organizations e.g., the ITU, ISO and the International Electrotechnical Commission (IEC). With time, standardization activity expanded to the two additional institutions i.e. *de facto* and governmental standardization bodies.¹⁰³ As in the telecommunications field, cyberspace is also subjected to all three, albeit not necessarily in that evolutionary order, as will be described in the following parts.

F. Conclusions

As shown, the absorption of high technology, through one or more standards, into ordinary usage in IT markets, i.e. cyberspace, is sequential. Generally, there are three consecutive independent technological phases, in the establishment of a standardized technology, beginning with the emergence of a technology in the development phase and ending in a full technological life cycle with the maturity and decline of the standardized technology in the

Information Technology Standards and Standardization: A Global Perspective (Kai Jakobs ed.) (2000) 19, pp. 30-31; For a description of gray standardization institutions, see, e.g., T. M. Egyedi, *supra* note 2, pp. 54-55; For one example of such activity, see, also, e.g., *the Bluetooth consortium*, a group of companies that has formed a "Special Interest Group" in order to develop standards for wireless connectivity for communications appliances, at: <www.bluetooth.com> (Last visited 28 August 2002).

¹⁰⁰ As typical ex-post legal concerns, these legal aspects will, largely, remain outside the scope of this study, which as explained earlier – wishes to focus on the standardization production process, generally seen as an ex-ante regulative constrain.

¹⁰¹ J. Farrell & G. Saloner, *supra* note 10, p. 4; R. T Nimmer, *standards, antitrust and Intellectual Property*, in *PLI/Intellectual Property-Antitrust* (1997); K. Lee, *Global Telecommunications Regulation: A Political Economy Perspective* (London, 1995) (for a description of the telecommunications field main precedents: the International Telecommunications User Group (INTUG), Intelsat or Eutelsat), pp. 121-122; *Formal methods in standards: A report from the British Computer Society (BCS) working group* (C.L.N Ruggles ed.) (London, 1990) (for a broad description of the various early European and American-based International standardization organizations), pp. 7-8.

¹⁰² E.g., R. T Nimmer, *Ibid*, id.

¹⁰³ P. Mähönen, *The Standardization Process in IT – Too Slow or Too Fast?*, at *Information Technology Standards and Standardization: A Global Perspective* (Kai Jakobs, eds) (Idea Group Publishing 1999) 35, p. 37.

termination of the implementation phase. Next to the conceptual variation in the technological phases, standards and thus, standard setting activity varies, accordingly, in space, with the partition of cyberspace's standardized architecture into four layers. Broadly, one can draw a clear distinction between the first three system-oriented layers on the one hand, and the fourth user-oriented layer on the other hand - these two groups of layers consist substantively different technological standards, and in accordance also different regulative costs and concerns:

First, the three lower layers imbed infrastructure standards, made to maintain expensive lines¹⁰⁴, through data networking equipment¹⁰⁵, Internet backbone telecommunications and cable services, intended to carry traffic.¹⁰⁶ As seen, this type of standard is most common to the, typically, early development phase. Second, the latter application layer, which involves a substantively different type of standards: namely, application standards, which establish most of cyberspace's computer software products, and are to be found primarily in the following implementation phase of IT standardization activity, such as in cyberspace.

Once conceptual different phases of technological development, and in accordance, different technological standards are recognized - a rational policy-maker should be able to predict efficiently, the degree of regulative compliance of each such standardized technology with typical price based Kaldor-Hicksian efficiency, if at all. This in his or her way to establish a comprehensive regulative policy. Based on that, any optimal institutional choice will have to be met along the following three technological phases, upon their distinctive standardization activity.

V

THE IMPLEMENTATION PHASE: THE RISE OF AUTONOMOUS INSTITUTIONS

[...]

D. A potential deviation: The ICANN case study

One potential deviation from the supported general policy for infrastructure standard setting came in the form of the federal government's involvement with the Internet Corporation for Assigned Names and Numbers (ICANN) 'domain name system' - the naming hierarchy that in

¹⁰⁴ But lots of cheap routers that manage a limited number of (these expensive) lines. See, e.g., J. K. MacKie-Mason & H. R. Varian, *Pricing the Internet, In Public Access to the Internet* (B. Kahin & J. Keller eds.) (estimating that this conclusion is reflected in the rapid decline from expensive routers to expensive transmission links), p. 273.

¹⁰⁵ Both oriented at clients (modem, ISDN, cable) and servers (routers, modem pools, and call aggregators).

¹⁰⁶ E.g. hybrid fiber-coax to cable and digital cable for higher-speed PC Internet connections.

essence tells connected computers where to find particular web sites. Eventually, the government did transfer a mandate on managing the authority to a private nonprofit (California) corporation. ICANN was appointed to oversee the operation of the root server system. In this capacity it was delegated to support existing protocols and telecommunications services used to implement domain name facilities.¹⁰⁷ For that purpose, ICANN board of directors received two different functions. The first, taking steps towards introducing competition into the Domain Name registration system. The second was to uphold a policy against cyber squatting through its Uniform Dispute Resolution Policy (the UDRP) and arbitration Panel.

As such, ICANN's establishment suggested two types of standardization concerns. The first lie in its potentially problematic institutional identity; with the second being its wide technical mandate as a standardization organization, as follows.

For a start, as a technical standardization institution, ICANN was initially constructed as a private interest group, as is evident from its structure, its insider consensus mechanism and its politically fractioned secretarial character.¹⁰⁸ Thus, as a private entity it exercises direct and central control – with the U.S. government choice to remain merely in the background.¹⁰⁹

As suggested earlier through public choice analysis – left alone, such competitive interest group might establish genuine public policy inefficiency. In addition, it might even create a monopoly on the allocation of the DNS's IP names and numbers.¹¹⁰ These latter challenges are not merely structural as they often interplay with ICANN's unique technological mandate:

Thus far, standardization concern is a function of ICANN's technical responsibilities. Arguably, ICANN was made responsible for potentially too broadly defined technical discretion, being it ICANN's blurry mandate on code writing i.e. technological standardization. Such as, the maintenance of the bit size of data packets, the architecture of the root services, i.e. assigning of IP numbers and the number and top-level domains that can safely be added to the Root, the preservation of unique protocol numbers for other various Internet functions, etc.

¹⁰⁷ On these facilities, see, generally, Domain Name, supra note 78, id; *Domain Name- Implementation and specification, Network Working Group*, RFC 883 at: <<ftp://ftp.isi.edu-notes/rfc883.txt>> (Last visited 28 August 2002).

¹⁰⁸ For critical literature on these governance policy issues, see, e.g., Michael A. Froomkin, *Wrong turn in cyberspace: Using ICANN to route around the APA and the constitution*, 50 Duke L. J. 17 (2000), pp. 160-165; Neil. W. Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 Cal. L. Rev. 395 (2000), pp. 484-487; Jonathan Weinberg, *ICANN and the problem of legitimacy*, 50 Duke L. J. 187.

¹⁰⁹ See, e.g., S. M. Benjamin et al., supra note 55, p. 825.

¹¹⁰ See, generally, A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust* (published on-line as a working paper) <<http://www.law.berkeley.edu/institutes/bclt/pubs/wp/202.pdf>> (last visited 28 August 2002) (Addressing the various potentially anti-competitive effects of ICANN), id; Michael A. Froomkin, supra note 111 (suggesting that the analyses of the privatization of the DNS and TCP/IP, highlight some of the reasons why the bottom-up process has failed), p. 216 et al.; Jay P. Kesav & Rajiv C. Shah, *Fool Us Once Shame on You – Fool Us Twice Shame on Us: What We Can Learn From the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 Wash. U.L.Q. 89 (2001) (suggesting that the Internet community was not able to resolve the uniformity problem through a bottom-up process, and, as a result, the U.S Government has begun to intervene), P. 214.

Originally, it was informally declared that: “the U.S. government should end its role in the Internet number and name address system”.¹¹¹ Instead the Department of Commerce initiated the White paper, which is a non-binding report statement of policy.¹¹² Like the ‘Green Paper’ statement of policy before it, the White paper has conformed to the already existing vague and basic governmental “Principles for a New System” as “stability¹¹³, competition, private bottom-up coordination, and representation”, with no clear separation between a technical standardization policy and non-technical (or even technical coordination) technical governance responsibilities.¹¹⁴ Accordingly, also the DoC characterized ICANN’s responsibility in blurred terms. This new corporation was made responsible only for “technical management of the DNS”, which was most likely undermined as the “narrow of management and administration of Internet names and numbers on an ongoing basis”. Overall, most commentators still agree that the U.S. government still holds de facto control of the root zone.¹¹⁵ However, it is also clear that the U.S. Government has chosen not to have direct control over the Root server.¹¹⁶

Thus far, the main controversy over ICANN’s governance mandate was mostly limited to the question of its democratic decision-making accountability. Consequently, the question of its technological standardization i.e. code writing mandate has still not been raised properly, as a separate policy question, thus undermining the need to decide on future technological risks, e.g. fragmentation of the network layer and the ultimate risk of Root splitting.¹¹⁷ To date, both ICANN and DoC deny that ICANN is engaged in either regulation or governance. Instead they hold out the general observation suggesting that ICANN is practically engaged in nothing more than ‘routine’ standard setting or presumably ‘technical coordination’ or ‘maintenance’.¹¹⁸ The need to confront these technological risks is not merely theoretical. Present infrastructure transparency concerns are already a good case in point for that:

¹¹¹ See, *Management of Internet Names and Addresses*, 63 Fed. Reg. 31,741 (1998) [Hereinafter, the White Paper] at <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm> (Last visited 28 August 2002), at 31, 749.

¹¹² Ibid, id.

¹¹³ Ibid, “...During the transition and thereafter, the stability of the Internet should be the first priority of any DNS management system...” at 31,743.

¹¹⁴ Compare: Michael A. Froomkin, supra note 108 (further suggesting that the DoC draws one henceforth), p. 171 et al.

¹¹⁵ Ibid (suggesting that “there is no dispute that the U.S. government, through the Department of Commerce, currently enjoys de facto control of the DNS”), p. 166; (adding that “Nor is there any dispute that DoC has at least temporarily ceded to ICANN, through a variety of contractual and quasi-contractual agreements, almost all the control the United States enjoys”), p. id; Steve Kettmann, *Will U.S. Release Grip on ICANN?* <<http://www.wired.com/news/infostructure/0,1377,49836,00.html>> (last visited 28 August 2002) (emphasizing that post September 11 the gradual process by which ICANN will gain autonomy from the government has been slowed), id.

¹¹⁶ Michael A. Froomkin, supra note 108, (suggesting that for that reason the U.S. government had, in fact, only quasi-privatized the control on the root server), p. 169

¹¹⁷ This "Split DNS" (or "two faced DNS"), is also a corollary of this same fragmentation, followed by the loss in communication between a particular FQDN and an IPv4 address, whenever it ceases to be universal and steady.

¹¹⁸ *The white paper*, supra note 111, at 31,744.

Broadly, infrastructure transparency was referred to as the original Internet concept of a single universal logical addressing scheme and the mechanisms by which packets may flow from source to destination essentially unaltered. Regrettably, much of this traditional end-to-end transparency infrastructure standard mechanism has been lost in the current Internet.¹¹⁹ That adds up to complexity in applications design and inhibits the deployment of new applications.¹²⁰ Overall, there are multiple causes for the loss of transparency i.e. the deployment of network address translation devices, the use of private addresses, firewalls and application level gateways, proxies and caches, etc.¹²¹ In recent years, as part of ICANN's appropriate concern with preserving end-to-end transparency, it became notably involved with the various issues surrounding internationalized domain name (IDN) standardization. Thus, ICANN's Board has begun to promote inquiries about that role and views with regard to the various efforts to use non-ASCII characters to design international domain names supported by the domain name system at large. Eventually, on 25 September 2000, the ICANN Board approved a set of resolutions (00.77 to 00.80) (formally relating to the 22 August Verisign Global Registry Services announcement about its introduction of the multilingual test bed), in which the Board recognized the importance of the Internet evolving to be more accessible to those who do not use the ASCII character set.¹²² Ultimately, ICANN recognized a need to specify an adequate standards track protocol based on supporting test bed findings and requirements. Upon final adoption IDNs would probably become fully operational in a standards-based way.¹²³ Consistent with ICANN's policy, the accepted standard would then have to be fully compatible with the Internet's existing end-to-end model, and 'preserve globally unique naming in a universally resolvable public name space'.¹²⁴

As the specially designed Internationalized Domain Names Committee has suggested, any TLD expansion should occur in a careful and controlled fashion, with regard for the overall stability of the DNS.¹²⁵ On balance, as long as the DNS is subject to the present pre-designed

¹¹⁹ IETF Network Working Group, at M. Kaat, *Overview of 1999 IAB Network Layer Workshop*, Network Working Group, RFC 2956 (October 2000), at: <<ftp://ftp.ietf.org/rfc/rfc2956.txt>> (Last visited 28 August 2002) ("Specifically the assumption that IPv4 addresses are globally unique or invariant is no longer true"), p. 2, § 2.1.

¹²⁰ Ibid ("It was however concluded that end-to-end transparency is desirable and is an important issue to pursue"), p.3 § 2.1.

¹²¹ Ibid, id.

¹²² See, Internet Corporation for Assigned Names and Numbers Minutes of Special Meeting (25 September 2000) <<http://www.icann.org/minutes/minutes-25sep00.htm#MultilingualDomainNames>> (Last visited 28 August 2002), upheld also at: Internationalized Domain Names Internal Working Group (of the Board), <<http://www.icann.org/committees/idn/iwg-15nov01.htm>> (last visited 28 August 2002).

¹²³ Thus, de facto designers of browsers or other Internet software would then be able to program their software to convert any foreign-character domains typed in or linked to into the appropriately coded string, which could then be resolved using normal DNS queries.

¹²⁴ See, Internet Corporation for Assigned Names and Numbers Minutes of Special Meeting supra note 269, upheld also at: Internationalized Domain Names Internal Working Group (of the Board), id.

¹²⁵ On the fundamental importance for DNS stability, see, e.g., *Internationalized Domain Names (IDN) Committee Discussion Paper on Non-ASCII Top-Level Domain Policy Issues* <<http://www.icann.org/committees/idn/non-ascii-tld-paper.htm>> (Last visited 28 August 2002) (warning that "(2) the sudden introduction of a massive number of new TLDs would be a bad idea"); See, also, IETF Network Working Group, at M. Kaat, supra note 119 ("Operational stability of DNS is paramount... It is therefore recommended to the IETF that, except for those changes that are already in progress and will

scarcity policy, that stability will be achieved within the limit of the total number of TLDs eligible for delegation to a given geographic unit.¹²⁶ IDNs should, therefore be carefully and agreeably set at a number equal to the number of its official languages. In part, this technological challenge was met successfully. However, it took more than a quasi-privatized ICANN to do so, as ICANN asked for the legitimacy and intervention of ISO. Technically, the ISO-3166-1 IDS table developers at ISO, appointed earlier by ICANN, already solved the problem of what is and is not a recognized geographic unit (country or geographically distinct territory).¹²⁷ However, being it a sensitive politically oriented decision, the table only provides two- and three-letter ASCII codes for each such geographic unit. Thus, ISO's table does *not* solve the multi-facet problem of what non-ASCII names (or abbreviations) should be assigned to each recognized geographic unit, and who should be in charge of assigning them. That politically oriented question is now still open.

In essence, the current ICANN/IANA policy permits the delegation of ASCII ccTLDs only when a given geographic unit and its associated specific 2-letter ASCII codes appear on the ISO 3166-1 list. Due to the heavy political nature of this question, ICANN/IANA's policy has so far failed to authorize so with non-ASCII characters, leaving ICANN without a given reference point for IDNs.

support easier renumbering of networks and improved security, no fundamental changes or additions to the DNS be made for the foreseeable future”), p.10.

¹²⁶ In regulation analysis, any definition of a regulative realm as scarce is of meaningful consequences; such is, arguably the case with the DNS (and IDNs) infrastructure, described above. For a political rather than technical explanation of DNS scarcity, see, e.g., Sharon Eisner Gillett & Mitchell Kapor, *The Self-governing Internet: Coordination by Design*, in *Coordination of the Internet*, edited by Brian Kahin and James Keller (MIT Press, 1997) (“Scarcity is a key characteristic that distinguishes administrative from political processes...The IETF process has produced many proposals for change, but few (if any) have been implemented because of the perceived need for consensus, which is highly valued but notoriously slow to achieve”); See, also, David Randy Conard, *Personal communication with Randy Conrad of APNIC*, September 1996 (“The current mechanisms by which addresses are allocated fundamentally [rely] on trust...[T]he allocation authorities must trust the requesters to provide an accurate and honest assessment of their requirements in order for appropriate amounts of address space to be allocated and the requesters must trust the allocation authorities to be fair and even handed...[H]owever, with the rapid ascendancy of commercial networks on the Internet, the trust model for resource allocation is under severe pressure”), id. For a more technical explanation, see, Sharon Eisner Gillett & Mitchell Kapor, *ibid.* (concluding that “The bottom line is that uncertainty in the future growth rate combines with uncertain user adoption of technical changes make it impossible to predict whether there are enough IPv4 addresses to satisfy demand”, id.; See, also, David Randy Conard, *ibid.* (“The bottom line is that successful address allocation requires administrators with strong technical skills, not just political or legal expertise”), id. In practice, as Einer describes, DNS allocation is subject to two types of policies: First, “based on extrapolation of past growth rates, the registries feel compelled to allocate remaining IPv4 address space conservatively”, id. Second, acknowledging that allocation authorities are trying to simplify the Internet routing system, “registries prefer to allocate larger contiguous blocks of addresses, which are of course less plentiful than smaller blocks”, id. Consequently, this section's argument will depart from the assumption of DNS scarcity regulation, upon its institutional implications, *infra.*

¹²⁷ For most users of ISO 3166-1 the standard is the list of country names and codes. Background on *ISO 3166* <<http://www.iso.org/iso/en/prods-services/iso3166ma/04background-on-iso-3166/index.html>> (last visited 28 August 2002), id.

With the risk of overly-decentralizing the responsibility for the latter, there is still a potential peril that the ICANN Board would decide to delegate to each self-interested proposer the task of identifying the desired TLD string for each non-ASCII script and justify it subjectively. However, while enabling users to easily type domain names in familiar non-ASCII scripts - that decision might then curtail ICANN's new main goal of privatizing today's DNS universal uniqueness.

An additional derivative political problem is of identifying and achieving consensus among the stakeholders of a given set of language communities. Left to the 'market of nations', ICANN/IANA's hegemony might be facing self-interested competing claims backed by different stakeholders, or, worse, different national governments. Left alone, national registries would have an incentive to benefit their own customers on the expense of the DNS stability at large. Thus, maintaining such stability, in the face of growing self-interested commercial intervention, would be potentially a task poorly suited for a technical coordinating organization such as ICANN. Arguably, the quasi-privatized ICANN is now facing a set of political concerns for which it might not be well suited. Ultimately, ICANN might misuse its mandate of deciding when and to what neutral and authoritative arbiter should this problem be referred, thus risking potential DNS instability, both politically and ultimately technologically.

Alternatively, as the broadly agreed lowest common denominator rule, ICANN should attempt to enforce mandated policies only when there is a clear need for uniformity based on a substantive consensus among those who must implement such policies and are impacted by them.¹²⁸ But should have ICANN be faced with the challenge in the first place? With potentially little future agreement on the need for DNS uniformity, as in the case of IDNs, ICANN might be arguably approaching here its own institutional limits: Even assuming that in the longer run both economically and technically multiple language domain names are favorable – in the short-run, ICANN may still have to coordinate ad hoc undesired fragmentation that might weaken the stability of the DNS, and even destructive collusion between name owners. Inevitably, as a policy rule ICANN's Board may then have to be backed by more authoritative agents, namely formal industry standardization organization as with the case of ISO's 3166 Maintenance Agency¹²⁹; and in extreme scenarios of loss of DNS hegemony, even more notably by the DoC, and the U.S. government at large.

Here, as potentially elsewhere, seen narrowly as mere technological customary standard setting activity, no governmental guidelines were adequately established for ICANN, thus undermining the necessity for a visible and continuous technological standardization policy, at least when infrastructure standardization is directly concerned. Left as a technologically independent quasi-privatized standard setting organization, yet carrying public responsibility - an unmonitored ICANN may embed an underrated potential of designing or adapting standards unproductively.

¹²⁸ See, e.g., David R. Johnson and Susan P. Crawford, *The Idea of ICANN* <http://www.icannwatch.org/archive/the_idea_of_icann.htm> (last Visited 28 August 2002), id.

¹²⁹ As described earlier, so far, such partial intervention in ICANN's own mandate has already been made by the International Organization for Standardization (ISO) and its ISO 3166 Maintenance Agency.

VI CONCLUSIONS

In the future, cyberspace's change pattern is presumed to bring about new innovative developments, potentially as part of new technological generations.¹³⁰ Both the TCP/IP and the Internet, as a whole, will continue to be standardized, and standard setting will continue to shape new and existing cyber markets, at large. New protocols will be designed and old ones will be revised. As with analogous standardization regimes, there is the risk that unless the distinctive standardization policies will be seen en bloc, and thus sequential and context-based, cyberspace's largely successful institutional practice might not be preserved also prospectively.

With the growth in both the community of users and the demand for sophisticated applications - a more advanced standardized architecture is already needed. In part, new standardization challenges are already here - e.g., the ISO's new conceptual model and set of network protocols, known as the ISO/OSI (open system interconnected) protocols, which are potentially in line to replace part of the existing infrastructure, currently in use on the Internet,¹³¹ or the IP Version 6 (IPv6) which is designed to expand address space.¹³² Similarly, several external trends and influences are argued to have a large impact on the status of the infrastructure network layer, i.e. the deployment of wireless network technologies, mobile-networked devices and special purpose IP devices.¹³³ Leaving aside the question of whether these specific developments will lead to a generation leap or less – it is argued that any adoption of such

¹³⁰ See, e.g., the *Next Generation Internet (NGI)* U.S. federal initiative including experts from business, government and academia, trying to anticipate the next generation of Internet standardized applications. It was a three-year program, which started in 1996 with a \$300M that were divided among several government agencies (with the lead role going to DARPA). The program involved a test network with 100 sites that were linked at a speed 1,000 times greater than today for the design of revolutionary applications: at <http://www.ngi.gov/> (last visited 28 August 2002); and see especially the *Research Challenges for the Next Generation Internet Report*, produced by the NGI, at http://www.cra.org/Policy/NGI/research_chall.pdf (last visited 28 August 2002); For earlier IETF Network Working Group RFC's recommending various next generation revisions, see, e.g., *The recommendation for the IP next generation protocol*, RFC 1752, January 1995 at <http://www.ietf.org/rfc/rfc1752.txt> (last visited 28 August 2002) ; *Technical criteria for choosing IP: The next generation (Ipng)*, RFC 1726, Dec. 1994, at <http://www.ietf.org/rfc/rfc1726.txt> (Last visited 28 August 2002), id.

¹³¹ See, Ole Hanseth & Eric Monterio, *supra* note 2 (further explaining that new generations of infrastructure evolve by combining, extending and aligning existing infrastructure), p. 174 et al.

¹³² IPv6 was designed to replace the IPv4, as a long-term solution to limited 32-bit address space, which are 'only' more than 4 billion addresses. The address space of IPv6 is designed by 128 bits, so to include approximately $8 \cdot 10^{28}$ times bigger than the entire 32-bit address space. Floyd Wilder, *supra* note 16, pp. 155-164.

¹³³ See, e.g., Peter Brockmann, *User Demand for Internet Services: Is the Infrastructure Ready?*, *Computer Standards and Interfaces* 20 (1998) 117-121 (for a broader perspective on potential infrastructure trends); M. Kaat, *supra* note 119, § 1; See, also, *Programming Considerations for Developing Next-Generation Wireless Embedded Applications (white paper)* (January, 2002), at <http://www.itpapers.com/cgi/PSummaryIT.pl?paperid=29639&scid=421> (Last visited 28 August 2002) (describing compatibility challenges of future generation (2.5G and 3G) wireless systems); *OMAP: Enabling Multimedia Applications in 3G Wireless Terminals (white paper)* (December, 2000), at <http://www.itpapers.com/cgi/PSummaryIT.pl?paperid=29634&scid=421> (last visited 28 August 2002) (describing multimedia applications in third-generation (3G) wireless appliances), id.

central technologies, should follow this past two decades, by and large, positive experience of cyber standardization.

As for infrastructure standards, and notwithstanding strong governmental rhetoric concerning the need for regulative restraint and ICANN's potential inconsistency, this study generally supports the rationalization of the early central institutional adoption of a unified infrastructure set of standards for interconnective transmission i.e. TCP/IP. Justifiably, this early endeavor was not followed by private initiatives of creating a market for infrastructure standards for interconnectivity. Instead, only a market of telecommunications 'basic' services evolved, with the involvement of diverse infrastructure equipment providers including data networking equipment, Internet connections, telecommunications equipment providers, cable operators, etc. As described, mostly later on, a market for application standards was developed as well. In essence, even with the later creation of the market for backbone telecommunications services, a common stable denominator in the face of a governmental interconnective TCP/IP naturally monopolized standard and the consensual architecture were preserved. Hence, efficiently overshadowing the potential inter-institutional infrastructure standardization arms race minimization.

In retrospective, in this early development phase, only an ex-ante governmental standard setting initiative, delegated through its early federal agencies and followed by monitored activity regarding research institutions is inherently efficient. In this environment of poorly complied price-competition, the only exception, which should be gradually maintained is in giving away much of the government's power over the early market for carrying and access services, as was mostly done in the early 1990's. In essence, these infrastructure standard-setting activities had been primarily technically rather than commercially motivated. That policy eventually changed with its face towards commercialization of application and complementary standardized products. These central changes are what arguably led, among other things, to substantial competition in standard setting activity in cyberspace. In the future, such further changes could be expected to come, whenever such technological and economical developments take place, as part of future intermediate 'modification' phases.

Later in the process, that existing institutional choice should, once again, change towards future 'implementation' phases. In this phase of application and complementary standardization, apart from the limited indirect support for infrastructure routine standard setting activity of the present phase, e.g. increase in bandwidth on the backbone transmissions links, better physical access from homes and businesses etc. - political institutions i.e. the U.S. governments through its delegated agencies, and particularly the FCC, should stick to a restrained indirect role in its standardization activity, due to what are its institutional barriers on efficient participation. As a general matter, such policy should also facilitate essential competition among autonomous standard setting institutions.

In practice, while the conduit has neither at all times been lucid, nor followed one route, the telling of governmental understanding of the public interest in the United States revealed a positive and definite prototype of declining interference, notwithstanding an increasing number of such institutional sources.

Of special importance for this commercial environment is the role of autonomous industry institutions. As explained, due to new risks of ex-ante technological stagnation and/or ex-post anti-competitive effects, assimilated mainly with the lack of compatibility or convergence, on the one hand, and the need to sustain private competition on the other hand - a role for an industry voluntary regulative approach in formalizing gray and de facto standardization will turn to be essential.

By the same token, in future technological implementation phases, an industry is, arguably, the most efficient in chilling direct governmental incentives for intervention beforehand or ex-post. This is subject only to indirect governmental supervision rules, which facilitate market production of standards and procedural regulative intervention.

Although much of these policies are, and were, upheld in practice - so far the U.S. government or the FCC drew no sufficiently clear or comprehensive policy on the matter;¹³⁴ leaving institutional choice in the net's standardization subject to overly general principles of marketplace competition, made to assure 'reliability, interoperability, ease of use and scalability',¹³⁵ dependable of its general anti- government tone.

Even for specific infrastructure standardization, where the unspecified governmental rhetoric is erroneously king, potential risks of deviation from its justified pro-active practices, already suggests policy conformity. One important case study for such potential digression came in the form of federal governmental involvement with the ICANN Internet Corporation for Assigned Names and Numbers. Here as well, the question of technological standardization was not raised properly ex-ante as a policy question, thus undermining the need to confront upcoming technological threats, e.g. fragmentation of the network layer and even Root splitting. In addition, such policy made no adequate division between infrastructure standards and application standards for matters of regulative intervention, hence providing ICANN, as a potentially self-interested interest group, overly broad control over both, but especially over the former.

Indeed, ICANN's technical mandate reaches potentially much further than is literally understood from existing formal declarations. Seen narrowly as mere technological 'routine' standard setting through technological 'maintenance', no adequate governmental guidelines were put in place, thus undermining the necessity for a comprehensive technological policy already for the present ICANN and ultimately for the future.

¹³⁴ For a relevant early U.S. Federal warning about such a possibility, see, the *Bayh-Dole Patent Act of 1980, 15 U.S.C.A.* (Commerce and Trade part 63—Technology innovations) § 3701(8) (Main volume 1997) (declaring that "No comprehensive national policy exists to enhance technological innovation for commercial and public purposes. There is a need for such a policy, including a strong national policy supporting domestic technology transfer and utilization of the science and technology resources of the Federal Government"), id

¹³⁵ For the specific context of standard setting, see, *The Report*, supra note 16, § 9. For all-Internet purposes, see, *Ibid*, the *Bayh-Dole Patent Act of 1980*, § 3701(2), (9)-(11).

END OF DOCUMENT